

Attachment 1

Accompanying Statement Explaining how Teledigicom Corporation's Operating Procedures Ensure Compliance with the FCC's CPNI Rules

Teledigicom Corporation ("the Company", Form File ID: 830174) has established policies and procedures adequate to ensure compliance with Section 222 of the Communications Act of 1934, as amended, and with the Federal Communications Commission's ("the Commission") rules pertaining to customer proprietary network information ("CPNI") as set forth in section 64.2001-64.2011 of the Commission's rules. This statement summarizes the Company's policies and procedures designed to safeguard CPNI.

1. The Company may not use, disclose or permit access to CPNI without obtaining prior customer approval except as follows:
 - a. Where required by law (e.g., under a lawfully issued subpoena).
 - b. To initiate, render, bill, and collect for its telecommunications services.
 - c. To protect the Company's rights or property and/or to protect its users or other carriers from fraudulent, abusive, or the unlawful use of, or subscription to, such services.
 - d. To market additional services to customers that are within the same categories of service to which the customer already subscribes.
 - e. To market services formally known as "adjunct-to-basic" services.
2. The Company does not disclose or permit access to CPNI to trace customers that call competing service providers.
3. The Company trains all employees in an effort to ensure that they understand:
 - a. what CPNI is;
 - b. what the Company's obligations to protect CPNI are; and
 - c. when they are and are not authorized to use CPNI.

The Company also restricts employee access to customer information and call data and has an express disciplinary process in place for violation of the Company's policies and procedures. Violations may result in disciplinary action, up to and including termination.

The Company has also designated a CPNI Compliance Officer who is responsible for:

- a. communicating with the Company's attorneys and/or consultants regarding CPNI responsibilities, requirements and restrictions;
- b. supervising the training of Company employees and agents who use or have access to CPNI;
- c. supervising the use, disclosure, distribution or access to the Company's CPNI by independent contractors and joint venture partners;
- d. maintaining records regarding the use of CPNI in marketing campaigns; and

- e. receiving, reviewing and resolving questions or issues regarding use, disclosure, distribution or provision of access to CPNI.
- 4. Prior to allowing access to customers' CPNI to joint ventures or independent contractors, the Company will require each partner's entry into a confidentiality agreement and shall obtain opt-in approval from each customer whose CPNI would be disclosed.
- 5. The Company maintains a record of its sales and marketing campaigns that use its customers' CPNI. The Company will maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record will include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. Records will be maintained for a minimum of one year.
 - a. Prior to the commencement of a sales or marketing campaign that utilizes CPNI, the Company will establish the status of a customer's CPNI approval. Sales personnel must obtain supervisory approval from the CPNI Compliance Officer for any proposed outbound marketing request for customer approval.
 - i. Prior to any solicitation for customer approval, the Company will notify customers of their right to restrict the use of, disclosure of, and access to their CPNI in accordance with the Commission's rules set forth in 47 C.F.R. §64.2008.
 - ii. The Company will use opt-in approval for any instance in which the Company must obtain customer approval prior to using, disclosing, or permitting access to CPNI, except for those few instances in which no customer approval is required or in which the use of Opt-Out or One-Time approval is permitted.
 - iii. A customer's approval or disapproval remains in effect until the customer revokes or changes such approval or disapproval.
 - 1. Records of approvals are maintained for at least one year.
- 6. The Company has implemented a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI.
- 7. The Company may, after receiving an appropriate written request from a customer, disclose or provide the customer's CPNI to the customer by sending it to the customer's address of record. Any and all such customer requests:
 - a. must be made in writing;
 - b. must include the customer's correct billing name and address and telephone number;
 - c. must specify exactly what type or types of CPNI are to be provided;
 - d. must specify the time period for which the CPNI must be provided; and
 - e. must be signed by the customer.

The Company will disclose CPNI upon affirmative written request by the customer to any person designated by the customer, but only after the Company calls the customer's telephone number of record and/or sends a notification to the customer's address of record to verify the accuracy of this request.

8. The Company authenticates all telephone requests for CPNI through one of the following means:
 - a. the customer must furnish a pre-established password or the correct answer to back-up "shared secret" questions;
 - b. the Company will send the requested information to the customer's postal or electronic address of record; or
 - c. the Company will call the customer back at the customer's telephone number of record with the requested information.
9. The Company may permit customers to establish online accounts, but will require an appropriate password to be furnished by the customer before he or she can access any CPNI in his or her online account.
10. The Company may use a back-up method to confirm the identity of a customer. The back-up method will consist of a "shared-secret" combination of two pre-selected questions by the Company and two pre-selected answers by the customer.
11. Customer passwords and "shared-secret" information used for the back-up identification method must not be based upon readily available biographical information or account information.
12. The Company will retain all customer passwords and "shared secret" question- answer combinations in secure files that may be accessed only by authorized Company employees who need such information in order to authenticate the identity of customers requesting call detail information over the telephone.
13. Electronic files and databases containing CPNI may only be accessed by authorized Company employees who have been provided a currently effective strong password.
14. The Company will notify customers immediately whenever any of the following account details are created or changed:
 - a. password;
 - b. customer response to a back-up means of authentication for lost or forgotten passwords;
 - c. online account; or
 - d. address of record.

The notification will not be required when the customer initiates service.

The Company may provide notification of account changes through the following methods:


- a. calling the customer's telephone number of record and speaking directly with the customer or leaving a voicemail message;
- b. sending a text message to the telephone number of record; or
- c. mailing a notice to the postal or electronic address of record.
 - i. The notification must not be sent to the new account information.

The notification must not reveal the changed information.

15. The Company may negotiate alternative authentication procedures for services that the Company provides to business customers to whom the Company has assigned a dedicated account representative and for whom the Company has implemented specific identity confirmation requirements.
16. The Company will maintain appropriate paper and/or electronic records of customer approvals – whether oral, written, or electronic – for use, disclosure, or permitting access to individual CPNI. These records will include: (i) the date(s) of any and all of the customer's deemed Opt-out approvals and/or Opt-in approvals, together with the dates of any modifications or revocations of such approvals; and (ii) the type(s) of CPNI use, access, disclosure and/or distribution approved by the customer.
17. The Company annually submits a CPNI certification to the Commission from an officer with personal knowledge of the policies and procedures that it has implemented to safeguard CPNI.
18. The Company will provide written notice within five (5) business days to the Commission of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.
 - a. The notice will be in the form of a letter, and shall include the carrier's name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether the relevant state commission(s) has been notified and whether it has taken any action, a copy of the notice provided to the customers, and contact information. Such notice will be submitted even if the Company offers other methods by which customers may opt-out.
19. The Company will provide an initial notification to law enforcement and a subsequent notice to the customer (upon completion of the process of notifying law enforcement) if a security breach results in the disclosure of the customer's CPNI to a third party without the customer's authorization.
 - a. As soon as practicable (and in no event more than seven (7) days) after the Company discovers that a person (without authorization or exceeding authorization) has

intentionally gained access to, used or disclosed CPNI, the Company will provide electronic notification of such breach to the United States Secret Service and Federal Bureau of Investigation via a central reporting facility accessed through a link maintained by the FCC: <http://www.fcc.gov/eb/cpni>.

- b. The Company will maintain a record of any breaches discovered, notifications made to the US Secret Service and the FBI, and notifications made to customers. The record will include the dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. Such records will be maintained for a minimum of 2 years.
20. The Company takes reasonable measures to discover and protect against activity that is indicative of pretexting including requiring Company employees and agents to notify the CPNI Compliance Officer immediately by voice, voicemail or email of: (a) any suspicious or unusual call requesting a customer's call detail information or other CPNI; (b) any suspicious or unusual attempt by an individual to change a customer's password or account information (including providing inadequate or inappropriate identification or an incorrect address of record, telephone number of record, or other significant service information; (c) any and all discovered instances where access to the Company's electronic files or databases containing passwords or CPNI was denied due to the provision of incorrect logins and/or passwords; and (d) any complaint by a customer of unauthorized or inappropriate use or disclosure of his or her CPNI. The CPNI Compliance Officer will request further information in writing, and investigate or supervise the investigation of, any incident or group of incidents that reasonably appear to entail pretexting.
21. The Company has not taken any actions against data brokers in the past year.
22. The Company does not have any information with respect to the processes pretexters are using to attempt to access CPNI.


Signature


Printed Name


Date


Title